CoNe Freiburg

IIF INSTITUT FÜR INFORMATIK FREIBURG

Systeme II

6. Die Vermittlungsschicht (Teil 2)

Thomas Janson°, Kristof Van Laerhoven*, Christian Ortolf°

Folien: Christian Schindelhauer°

Technische Fakultät

°: Rechnernetze und Telematik, *: Eingebettete Systeme

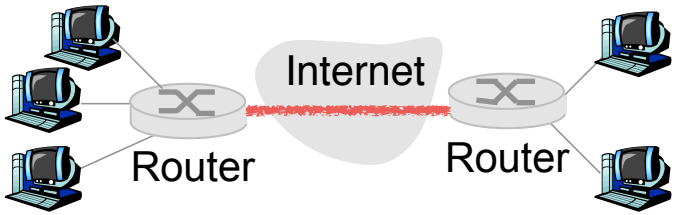
Albert-Ludwigs-Universität Freiburg

Version 24.04.2015

UNI FREIBURG

IPsec (RFC 2401)

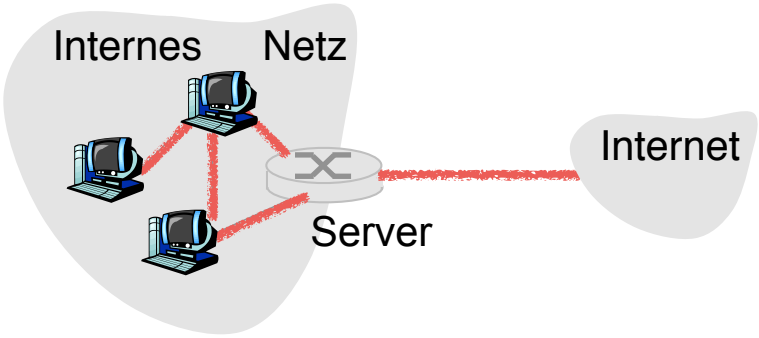
- Schutz vor Replay-Attacken
- IKE (Internet Key Exchange) Protokoll
  - Vereinbarung einer Security Association (SA)
  - Identifikation, Festlegung von Schlüsseln, Netzwerke, Erneuerungszeiträume für Authentifizierung
- Encapsulating Security Payload (ESP)
  - IP-Kopf unverschlüsselt, Nutzdaten verschlüsselt, mit Authentifizierung
- IPsec im Transportmodus (für direkte Verbindungen)
  - IPsec Header zwischen IP-Header und Nutzdaten
  - Überprüfung an den Endpunkten (dort muss IPsec vorhanden sein)
- IPsec im Tunnelmodus
  - Das komplette IP-Paket wird verschlüsselt und mit dem IPsec-Header in einen neuen IP-Header verpackt
  - IPsec muss nur an den Endpunkten (Router oder VPN-Gateway) vorhanden sein
- IPsec ist Bestandteil von IPv6
  - Rückportierungen nach IPv4 existieren

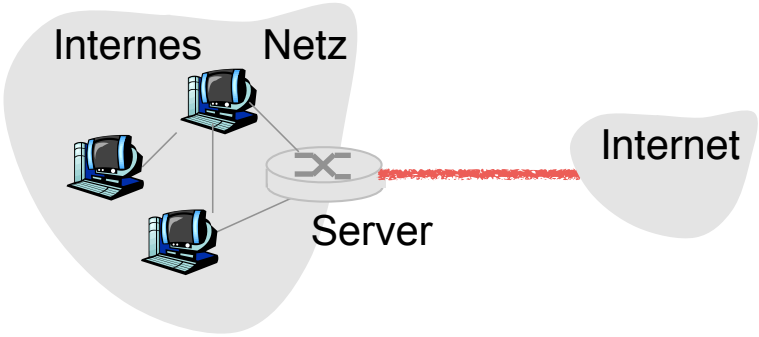


CoNe Freiburg

Firewalls

- Host-Firewall
  - z.B. Personal Firewall
  - kontrolliert den gesamten Datenverkehr eines Rechners
  - Schutz vor Attacken von außerhalb und von innen (Trojanern)
- Netzwerk-Firewall
  - unterscheidet
    - Externes Netz (Internet - feindselig)
    - Internes Netz (LAN - vertrauenswürdig)
    - Demilitarisierte Zone (vom externen Netz erreichbare Server)





CoNe Freiburg

Firewalls - Methoden

- Paketfilter
  - Sperren von Ports oder IP-Adressen
  - Content-Filter
  - Filtern von SPAM-Mails, Viren, ActiveX oder JavaScript aus HTML-Seiten
- Proxy
  - Transparente (extern sichtbare) Hosts
  - Kanalisierung der Kommunikation und möglicher Attacken auf gesicherte Rechner
- Honeylinks (nach Honeypot-Konzept)
  - Firewall eines Webservers injiziert versteckte HTML-Links auf nicht existierende Seiten
- Network Address Translation (NAT), Port Address Translation (PAT)
  - Geräte in lokalem Netz (LAN) nach außen nicht sichtbar
- Bastion Host
  - besonders gesicherter Rechner in demilitarisierter Zone, z.B. Proxy, Router

CoNe Freiburg

Firewalls: Begriffe

- (Network) Firewall
  - beschränkt den Zugriff auf ein geschütztes Netzwerk aus dem Internet
- Paket-Filter
  - wählen Pakete aus dem Datenfluss in oder aus dem Netzwerk aus
  - Zweck des Eingangsfilter:
    - z.B. Verletzung der Zugriffskontrolle
  - Zweck des Ausgangsfilter:
    - z.B. Trojaner
- Bastion Host
  - ist ein Rechner an der Peripherie, der besonderen Gefahren ausgesetzt ist
  - und daher besonders geschützt ist
- Dual-homed host
  - Normaler Rechner mit zwei Interfaces und IP-Adressen
  - verbindet Netzwerke, z.B. Internet und LAN

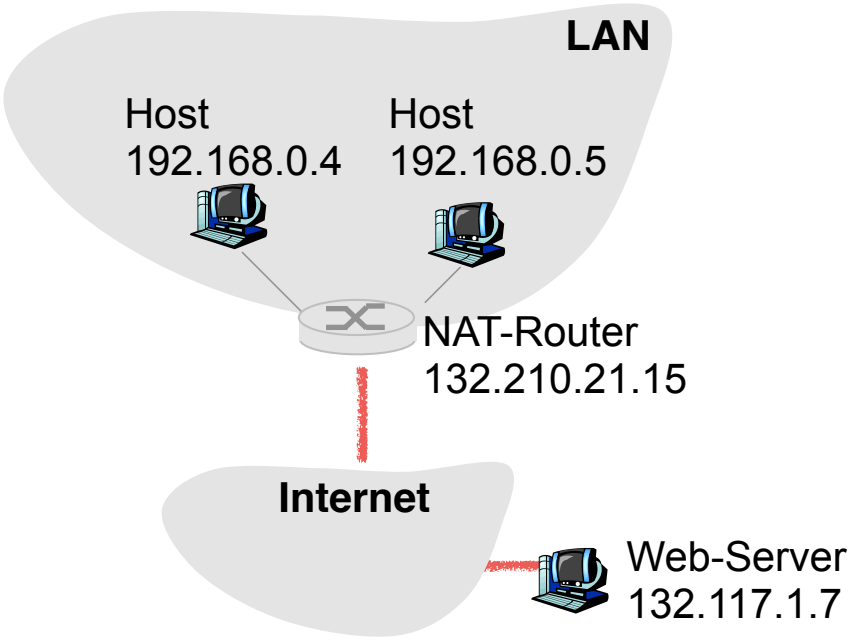
CoNe Freiburg

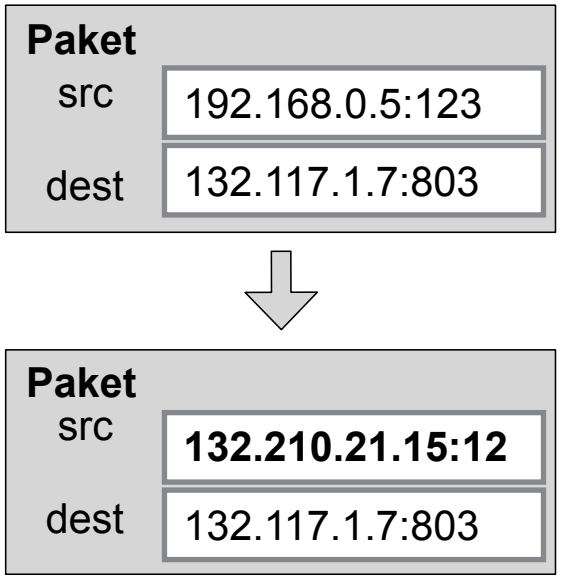
Firewalls: Begriffe

- Proxy (Stellvertreter)
  - Spezieller Rechner, über den Anfragen umgeleitet werden
  - Anfragen und Antworten werden über den Proxy geleitet
  - Vorteil
    - Nur dort müssen Abwehrmaßnahmen getroffen werden
- Perimeter Network:
  - Ein Teilnetzwerk, das zwischen gesicherter und ungesichter Zone eine zusätzliche Schutzschicht bietet
  - Synonym demilitarisierte Zone (DMZ)

NAT und PAT

- NAT (Network Address Translation)
- Basic NAT (Static NAT)
  - Jede interne IP wird durch eine externe IP ersetzt
- PAT (Port Address Translation) = NAPT (Network Address Port Translation)
  - Umkodierung von Socket-Paar (IP-Adresse und Port)
- UPnP (Universial Plug and Play): Router anweisen Ports zu konfigurieren
- Hole Punching (für IP-Telefonie, Peer-to-Peer-Netzwerke)





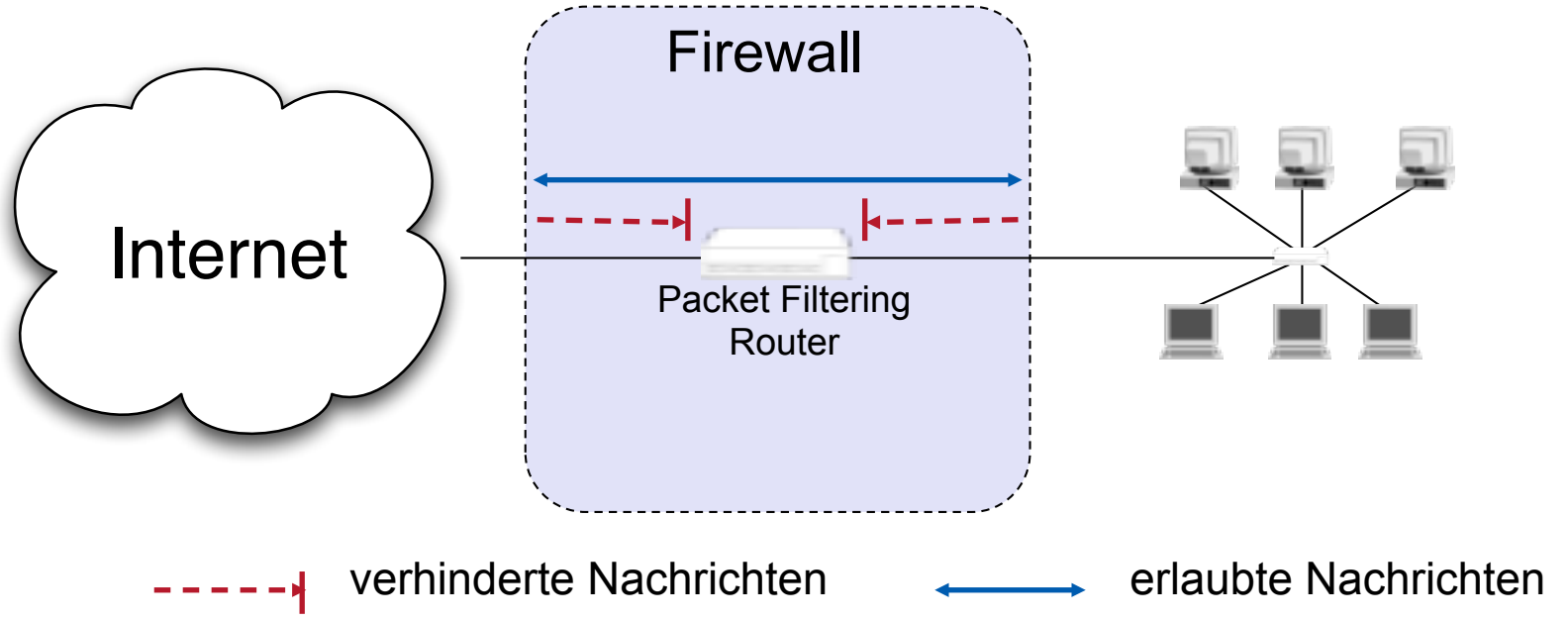
CoNe Freiburg

NAT und PAT

- Verfahren
  - Die verschiedenen lokalen Rechner werden in den Ports kodiert
  - Diese werden im Router an der Verbindung zum WAN dann geeignet kodiert
  - Bei ausgehenden Paketen wird die LAN-IP-Adresse und ein kodierter Port als Quelle angegeben
  - Bei eingehenden Paketen (mit der LAN-IP-Adresse als Ziel), kann dann aus dem kodierten Port der lokale Rechner und der passende Port aus einer Tabelle zurückgerechnet werden
- Sicherheitsvorteile
  - Rechner im lokalen Netzwerk können nicht direkt angesprochen werden
  - Löst auch das Problem knapper IPv4-Adressen
  - Lokale Rechner können nicht als Server dienen
- DHCP (Dynamic Host Configuration Protocol)
  - bringt ähnliche Vorteile

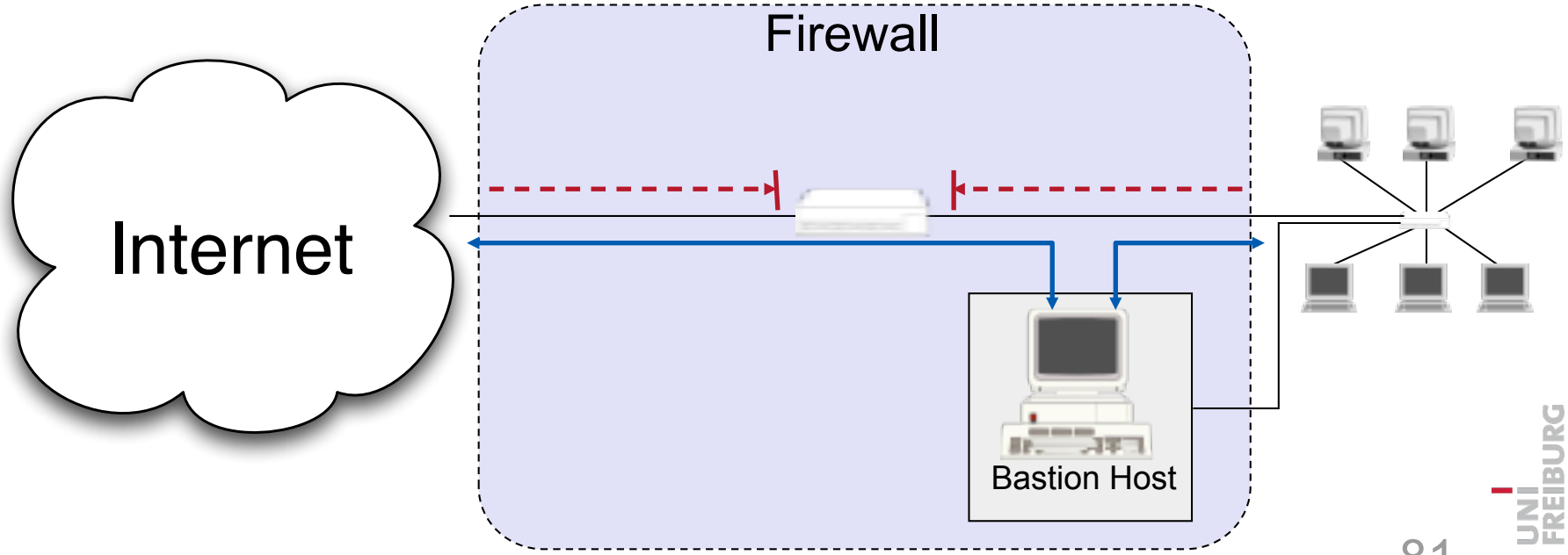
Firewall-Architektur Einfacher Paketfilter

- Realisiert durch
  - Eine Standard-Workstation (e.g. Linux PC) mit zwei Netzwerk-Interfaces und Filter-Software oder
  - Spezielles Router-Gerät mit Filterfähigkeiten



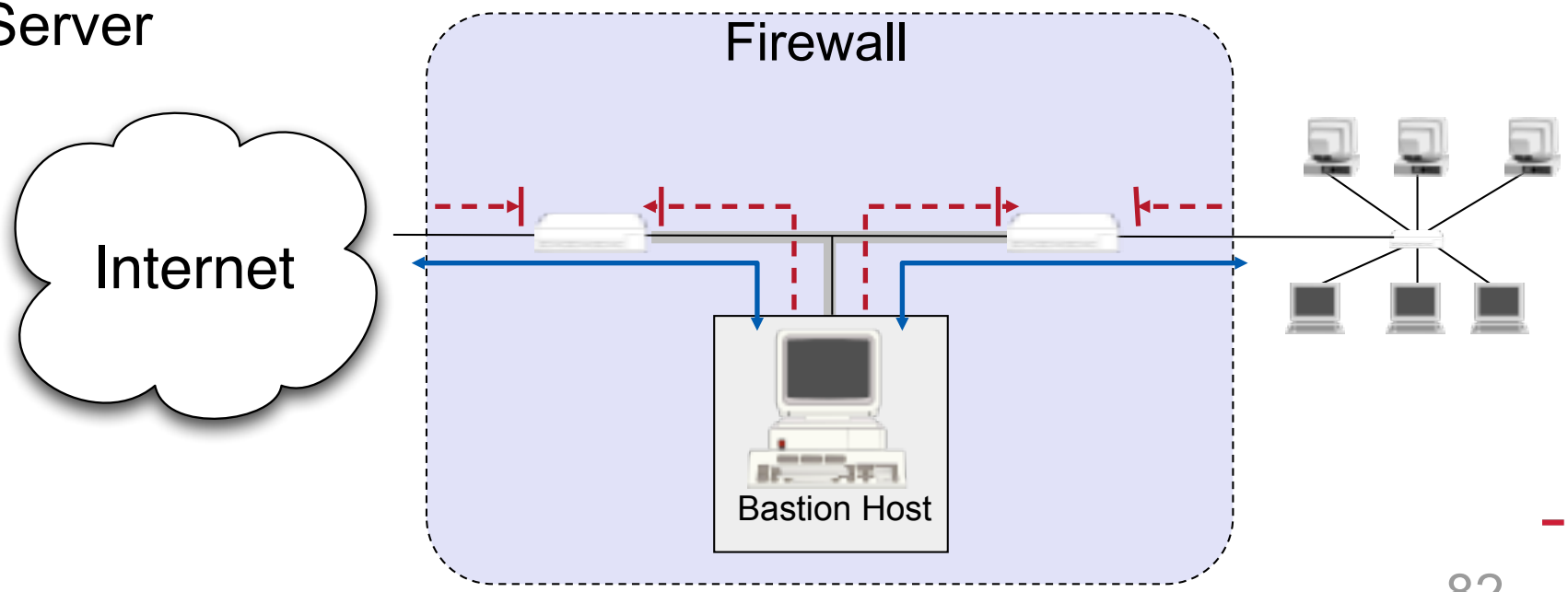
Firewall-Architektur Screened Host

- Screened Host
- Der Paketfilter
  - erlaubt nur Verkehr zwischen Internet und dem Bastion Host und
  - Bastion Host und geschützten Netzwerk
- Der Screened Host bietet sich als Proxy an
  - Der Proxy Host hat die Fähigkeiten selbst Angriffe abzuwehren



Firewall-Architektur Screened Subnet

- Perimeter network zwischen Paketfiltern
- Der innere Paketfilter schützt das innere Netzwerk, falls das Perimeter-Network in Schwierigkeiten kommt
  - Ein gehackter Bastion Host kann so das Netzwerk nicht ausspionieren
- Perimeter Netzwerke sind besonders geeignet für die Bereitstellung öffentlicher Dienste, z.B. FTP, oder WWW-Server



CoNe Freiburg

Firewall und Paketfilter

- Fähigkeiten von Paketfilter
  - Erkennung von Typ möglich (Demultiplexing-Information)
- Verkehrskontrolle durch
  - Source IP Address
  - Destination IP Address
  - Transport protocol
  - Source/destination application port
- Grenzen von Paketfiltern (und Firewalls)
  - Tunnel-Algorithmen sind aber mitunter nicht erkennbar, z.B. RPC/HTTPS (Remote Procedure Call)
  - Möglich ist aber auch Eindringen über andere Verbindungen
    - z.B. Laptops, UMTS, GSM, Memory Sticks